NETWORK COMPROMISE RECOVERY METHODS AND APPARATUS

Abstract of the Disclosure

A secure communications system (100, FIG. 1) with a compromised communications node can quickly recover from the compromised condition by sending re-keying messages using a key encryption key hierarchy (200, FIG. 2). Each communications node (330, FIG. 3) includes a memory (300, FIG. 3) with a list of tier-group specific key encryption keys, and whenever a message arrives that is encrypted with a key encryption key in the list, the communications node decrypts the message. When the message includes a new traffic encryption key, the communications node has been re-keyed. Key encryption keys are managed hierarchically such that many communications nodes can be re-keyed with very few broadcast messages, thereby saving communications resources.